

Frontline stories from IR - A Comprehensive Approach to Threat-Informed Defense

Suk Paul – Cyber Security Strategist

The Workaday Life of the World's Most Dangerous Ransomware Gang

A Ukrainian researcher leaked 60,000 messages from inside Conti. Here's what they reveal.



INFRASTRUCTURE

- Trickbot (2020)
- Emotet (2021)
- CobaltStrike official license

SmartContracts?

ORGANIZATION 100+ STAFF



Managers

Coders

Testers

Administrators

Reverse Engineers

Pen-testers/hackers

Human Resources

Journalist

GO-TO-MARKET & BUSINESS MODEL

Hospitals & Healthcare providers

100M+ USD revenue

Double extortion

\$180M/Year



What's up out there?

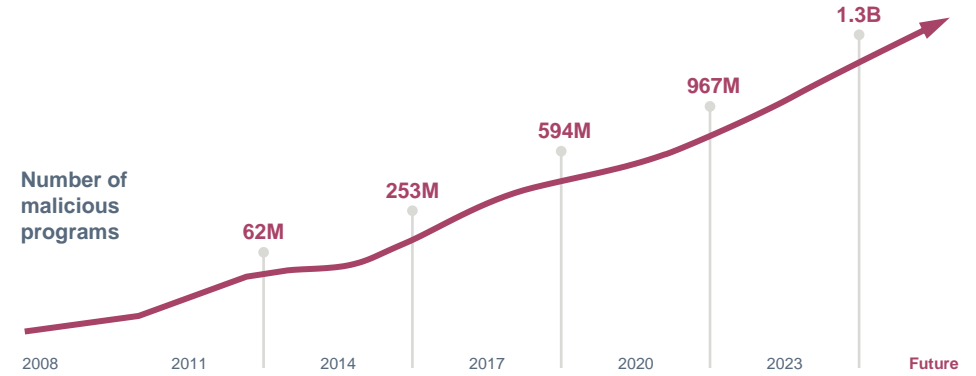


Time is the Enemy!



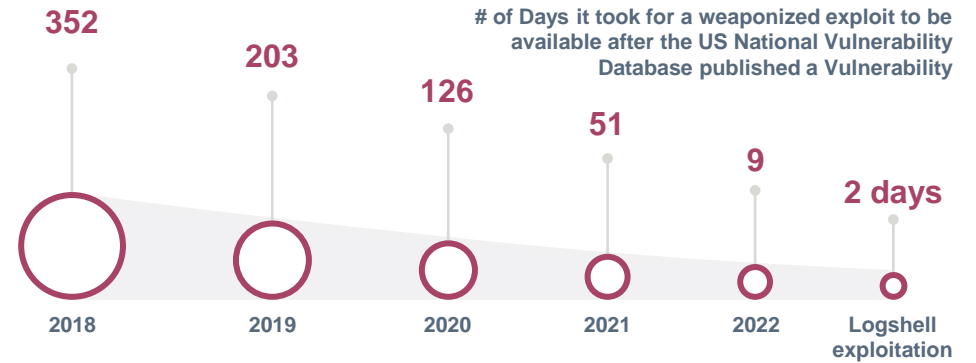
NUMBER OF MALICIOUS PROGRAMS SINCE 2014

20x increase



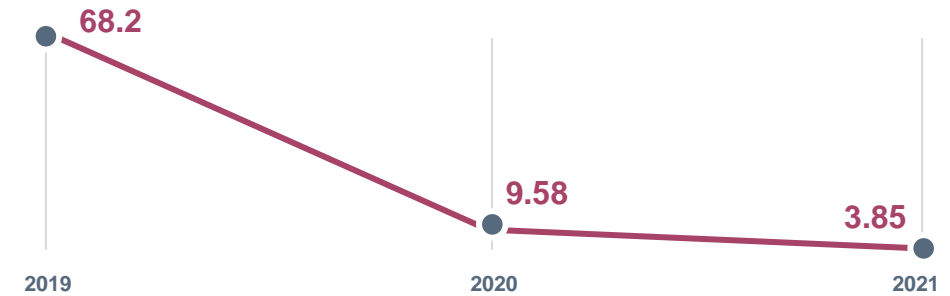
TIME TO WEAPONIZE EXPLOITS IN 2022

9 Days



AVG TIME BETWEEN THE FIRST EVIDENCE OF MALICIOUS ACTIVITY AND RANSOM REQUEST IN 2022

3.85 Days



Sources: AV Atlas IBM X-Force Intelligence, Gartner, Microsoft Digital Defense Report 2022

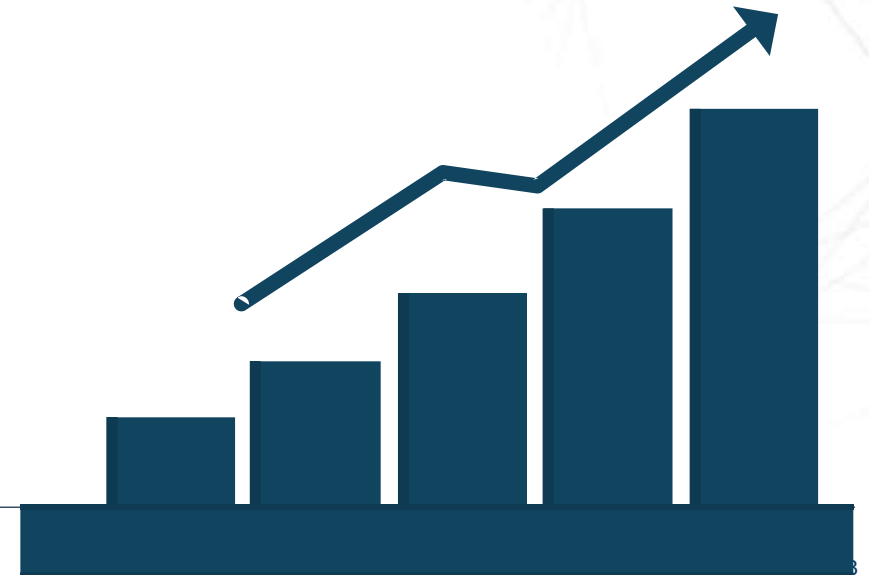
Trend 2023

Exceptional use of 0-days (66 to date)

Use of supply chain attacks

Use of cloud systems (exploitation or criminal infrastructure)

Use and infection of Operational Technology (OT) systems



Ransomware goes to Las Vegas!



\$100M in damages for the month of September alone! Exceeding the global average of \$4.5M*

Attack orchestrated by ALPHR (aka Blackcat)

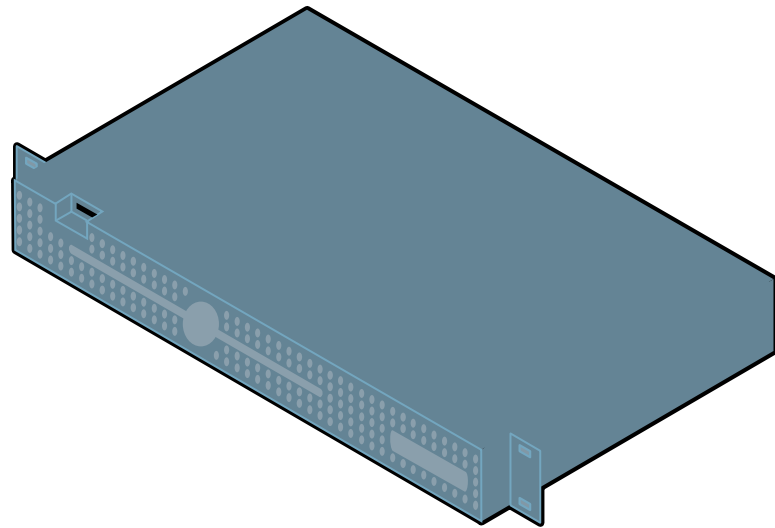
*Source: IBM Cost of a data breach report 2023

What we see from our **Cyber Fusion Centers**

- Standard attacks tactics still work (phishing, remote accesses, vulnerabilities), but different flavors
- 24x7 Detection prevents reaching the ransom stage
- EDR & NG AV services reduce the needs of Incident Response
- Penetration tests are generally not realistic, red team exercises more
- When hit by a large incident, crisis management is key

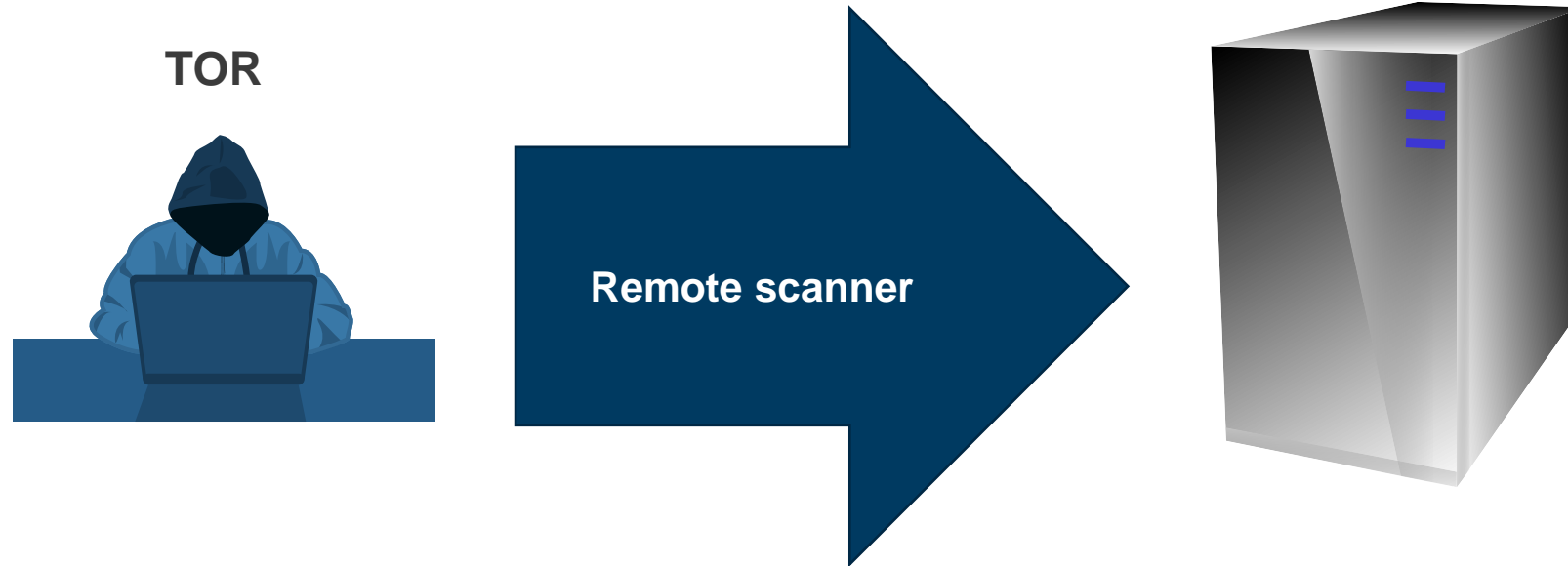
1. Ransomware incident

06h04: Alert escalated to Incident Response



1. Ransomware incident

06h36: Analysis of the brute force tentatives



1. Ransomware – Avoid pitfalls

Use of a local account with common passwords



**DISABLE LOCAL
ADMINISTRATOR ACCOUNTS**



**ONE-TIME PASSWORDS (E.G.
USING MICROSOFT LAPS
SOLUTION)**



**DEPLOYMENT OF A
PRIVILEGED ACCOUNT
MANAGEMENT TOOL (PAM)**

2. APT incident (state actor) One attacker can hide another



2. APT incident (state actor)

One attacker can hide another

Discovery of a threat actor in the perimeter of the client (APT 28)



2. APT incident (state actor) One attacker can hide another

Discovery of a 2nd group in the client's perimeter (APT 10)



2. APT Incident – Avoiding pitfalls

Do not rely solely on automatic alerts



**GENERATE HUNTING RULES
ADAPTED TO TTP**



**IMPLEMENT A 24/7
MONITORING SYSTEM AFTER
A COMPROMISE IS
DETECTED**



**CONDUCT REGULAR
COMPROMISE ASSESSMENTS**



Personal Data



Confidential Data



[Identify Person]

TIME TO PLAN

Name

Home Address

Business Address

Identity No

Passport No

Driving License

Income Tax No

Car Registration

Other



How to get protected ?



INTELLIGENCE



PREPARE



PROTECT



DETECT



RESPOND



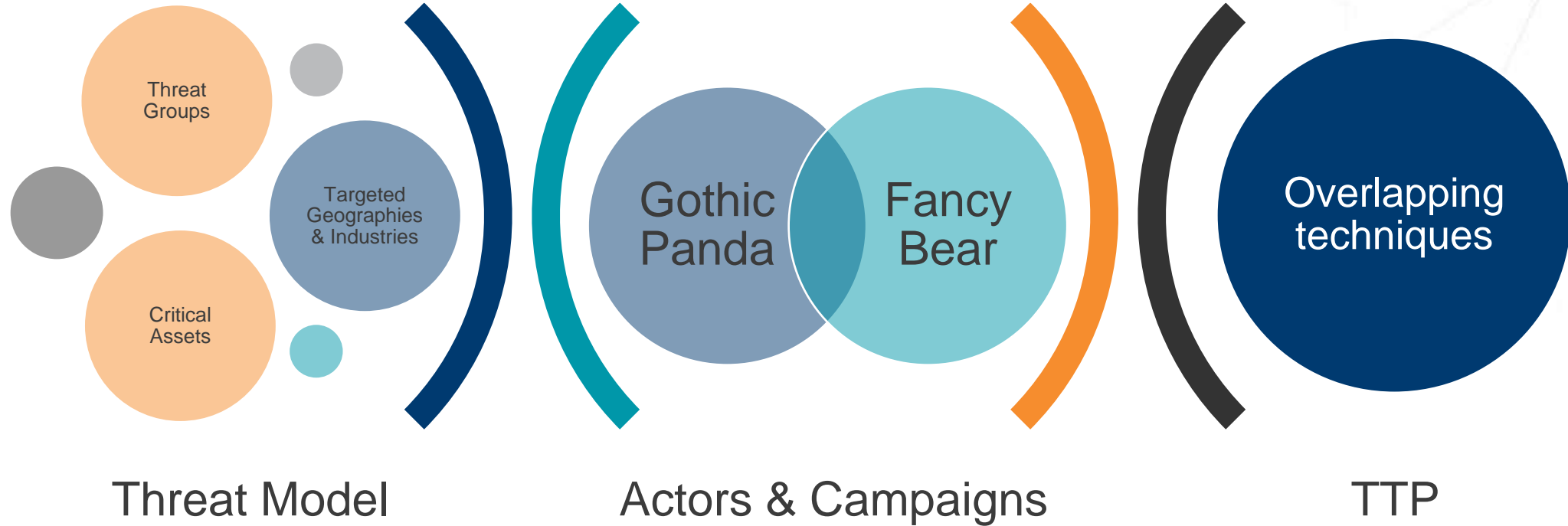
LEARN &
IMPROVE

GOVERNANCE

Know your enemy

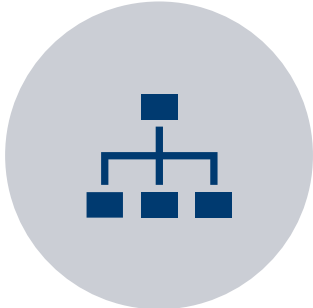


INTELLIGENCE



Plan your Security

ENABLED



BOARD
ACCOUNTABILITY



EMPOWERMENT



BUDGET



POLICIES

GOVERNANCE

KEY TAKEAWAYS

Know your enemy & threats – and prepare

Be 24x7 covered before, during and after an incident

Sniper and pragmatic methods pay back

Don't forget your horizontal coverage



Thank you

Suk Paul

Cyber Security Services Strategist
